November 16, 2018

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: **Ex Parte Presentation,** WC Docket No. 18-28, WC Docket No. 17-59, WT Docket No. 08-7, CC Docket No. 95-155

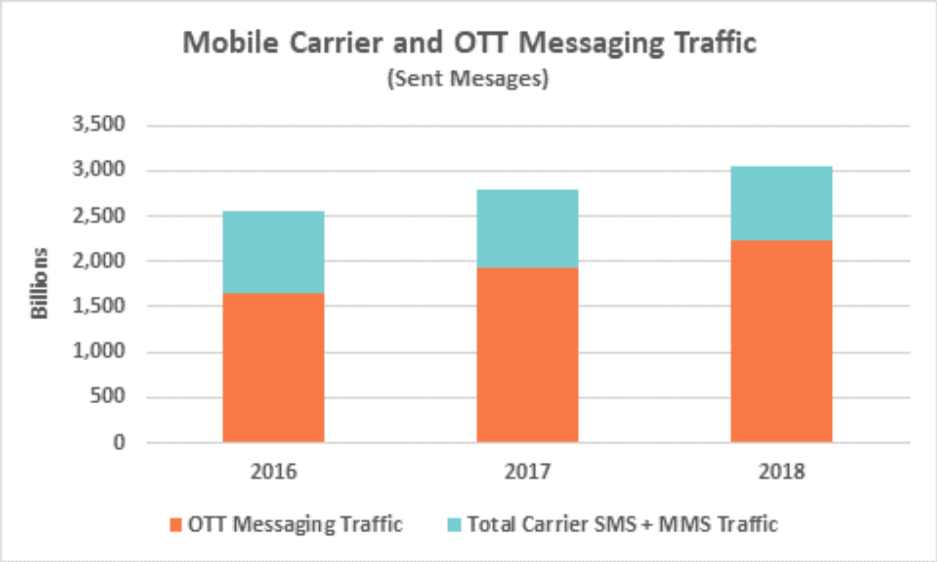
Dear Ms. Dortch,

On November 15, 2018, Scott Bergmann and Matthew Gerst of CTIA, together with outside counsel Adam Krinsky of Wilkinson Barker Knauer LLP, met with the following members of the Wireless Telecommunications Bureau: Suzanne Tetreault, Garnet Hanly, Elizabeth McIntyre, and by phone, Eli Johnson, Darrel Pae, Jennifer Salhus, and Becky Schwartz, to provide an overview and update on messaging services.

The Messaging Marketplace is Thriving and Competitive and Messaging is a Trusted Medium Due to Wireless Providers' Active Management

Messaging is a Thriving, Competitive Marketplace. Messaging is one of the most popular ways consumers communicate with friends, family and businesses. Year-over-year, the messaging market continues to grow and expand as consumers send more messages and new

service providers enter the ecosystem.[1] In 2018 alone, more than 3 trillion messages were sent, with OTT traffic accounting for almost triple the volume of SMS traffic.[2]



Source: Ovum

While consumer usage of SMS/MMS has remained relatively consistent over the last 3 years, the decline in SMS/MMS messaging from its peak has been attributed to the rise in competing OTT messaging platforms.[3]

Wireless Providers Work Diligently to Curb Spam and Unwanted Messages, and As a Result, Consumers Read Nearly All Messages (in Contrast to Email). It takes active management to maintain the current, spam-limited messaging environment and avoid a tidal wave of

[1] The messaging ecosystem generally includes wireless provider-offered SMS and MMS and over-the-top (OTT) messaging applications such as Apple's iMessage, WhatsApp, Facebook Messenger, Slack, Signal and Messenger by Google, to name a few.

[2] Pamela Clark-Dickson, Ovum, *Mobile Messaging Traffic and Revenue Forecast Report, 2017-22* (May 30, 2018), https://ovum.informa.com/resources/product-content/mobile-messaging-traffic-and-revenue-forecast-report-201722.

[3] *Id.*; *see also* Statista, *Most popular mobile messaging apps in the United States as of July 2018, by active users (in millions)*, at https://www.statista.com/statistics/350461/mobile-messenger-app-usage-usa/ (last visited Nov. 16, 2018).

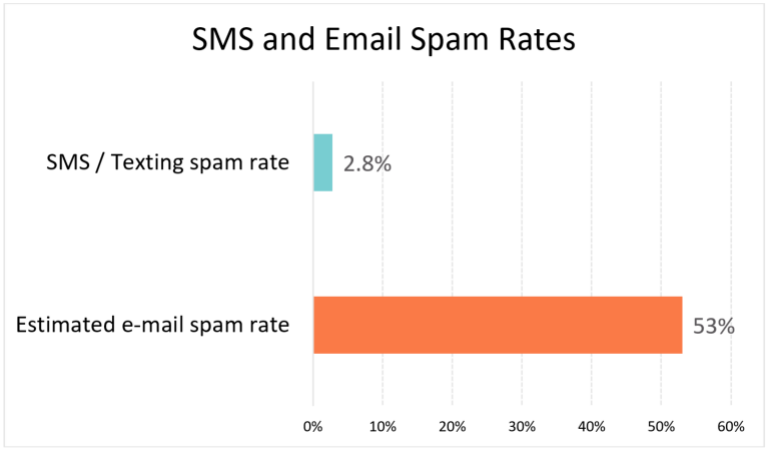
malicious and otherwise unwanted traffic from flooding the messaging ecosystem. For example, wireless providers apply filtering to prevent large volumes of unwanted messaging traffic or identify potentially harmful texts. Wireless providers also use "account fingerprinting" techniques to identify accounts sending high volumes of messages with key signs of spam activity.

Messaging's popularity is largely attributable to its status as a trusted and convenient communications environment. The fact that messaging continues to be a spam-limited environment is also a strong signal that CTIA's *Messaging Principles and Best Practices* are working to protect consumers from unwanted messages. Notably, the objectives of the *Messaging Principles and Best Practices* are to support a robust and dynamic wireless messaging community where:

- Wireless consumers can exchange wanted messages with other wireless consumers;
- Enterprises and consumers can exchange wanted messages; and
- Consumers are protected from unwanted messages, including in conformity with applicable laws and regulations, such as the Telephone Consumer Protection Act (TCPA).

Because of wireless providers' efforts consistent with the *Messaging Principles and Best Practices*, messaging remains a spam-limited environment and is a highly trusted medium – especially when compared to email. For example, the spam rate via SMS is estimated at 2.8 percent, compared to an estimated e-mail spam rate over 50 percent.[4]

[4] *See* Maria Vergelis, Nadezhda Demidova, and Tatyana Shcherbakova, Kaspersky Lab SecureList, *Spam and phishing in Q3 2018* (Nov. 6, 2018), https://securelist.com/spam-and-phishing-in-q3-2018/88686/ (global average email spam rate in Q3 2018 was 52.54 percent); Symantec, *Internet Security Threat Report, Email Threats 2017*, at 4, 6, 18 (Oct. 2017), available at https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf (spam accounted for 54 percent of email globally in the first half of 2017); *see also* Kim Fai Kok, Truecaller, *2018 U.S. Spam & Scam Report* (Apr. 26, 2018), https://blog.truecaller.com/2018/04/26/truecaller-insights-usa-2018/.



Note: The chart above is an illustrative representation of the Symantec, Kaspersky Lab and Truecaller estimates of email and SMS spam rates in 2017-2018.

To the extent these active consumer protection measures impact legitimate messaging traffic, wireless providers have taken steps to adjust and calibrate filters in real-time by utilizing global data from multiple sources and implementing rule-based decision-making, machine learning and artificial intelligence. In addition, wireless providers have directly partnered with message senders to "whitelist" traffic sent from verified legitimate senders. As the messaging ecosystem continues to innovate and evolve, wireless providers are also working to develop new tools and implement new technologies to delineate between legitimate and unwanted messaging traffic.

Wireless providers and messaging platforms are constantly evolving their efforts to protect consumers from being flooded with malicious and unwanted messages. As 25 state attorneys general have expressed to the Commission, the threat about scams conducted via messaging remains very real.[5] Thus, the Commission should enable providers throughout the messaging ecosystem to continue protecting consumers by supporting these industry-led and managed efforts.

[5] *See* Opposition of CTIA, WT Docket No. 08-7, at 12-18 (filed Nov. 20, 2015) (*CTIA Opposition*).

Messaging's Classification as an Information Service Enables Wireless Providers to Protect Consumers from Unwanted Messages

The Characteristics of Messaging Make It an Information Service. Like other asynchronous services such as email and voicemail, in which users send messages that are stored until the recipient accesses them, mobile messaging involves data storage and retrieval that are essential features of an information service. Further, text messaging involves computer processing that changes both the form and content of messages.[6]

A Telecommunications Service Classification Would Upend Wireless Providers' Active Management that is Successfully Restricting a Torrent of Unwanted Messages. The wireless industry is committed to delivering the messages consumers want and filtering out unwanted and malicious mass messages, and treating messaging as a telecommunications service would hamstring those efforts. It would allow spammers to bring endless challenges to filtering practices under Sections 201 and 202 of the Act, taking away critical flexibility to address evolving threats to consumers. It would jeopardize wireless providers' actions to filter spam and provide a safe consumer experience for mass messages. In contrast, an information service classification will provide certainty for wireless providers to apply consumer protection measures to keep messaging largely spam-free.

A Telecommunications Service Classification Would Impermissibly Subject Only a Subset of Messaging Providers – Wireless Providers – to FCC Regulation. Treating wireless providers' text messaging services as telecommunications services but not the growing range of OTT messaging applications and platforms (*e.g.*, WhatsApp, Facebook Messenger, Slack, and Signal) would undercut competitive and technical neutrality, especially when OTT messaging comprises nearly 75 percent of messaging traffic. Applying burdensome regulatory mandates exclusively to wireless providers' text messaging services would be arbitrary, risk distorting competition, and harm consumers' experience.

---

[6] *CTIA Opposition* at 34-42 ("SMS and MMS messages are subject to substantial computer processing and conversion").

Messaging is Not a Commercial Mobile Radio Service. To be a Commercial Radio Service (CMRS), a service must enable the capability to communicate with "all other users on the public switched network."[7] As CTIA has previously explained, messaging is not interconnected with users of the Public Switched Telephone Network.[8] For example, messaging generally does not allow communication with landline phones, and thus fails to meet this definition.

The fact that some text messages can be delivered to landlines by converting them into audio messages does not change this result. Text-to-Landline (TTL) is a service that is offered and priced separately from wireless providers' SMS/MMS messaging services.[9] TTL complements but is not itself text messaging,[10] and thus is not relevant to the analysis of text messaging's regulatory classification. As the Commission has stated, a CMRS classification assessment must "focus on the functions of the service itself rather than whether the service allows consumers to acquire other services that bridge the gap to the telephone network."[11] Much like broadband Internet access does not itself offer interconnection to the PSTN absent use of a distinct VoIP application, the availability of a TTL service does not transform wireless providers' SMS/MMS messaging services into an "interconnected" service.

Messaging is Not a "Functional Equivalent" of CMRS. FCC precedent establishes a presumption that a mobile service that is not CMRS is a PMRS, and that only a "very few"

---

[7] 47 C.F.R. § 20.3(a).

[8] *CTIA Opposition* at 43-44.

[9] Indeed, not all wireless providers offer TTL services and the vast majority of text messages are not sent using TTL capability. Moreover, some offerings enable TTL capability only to those landline numbers listed in the white pages and not to all landline numbers (*e.g.*, not to medical facilities, emergency operators, unlisted numbers).

[10] Further, TTL cannot transmit all of the content sent via messaging. For example, a voice message cannot usefully convey a photo or a clickable URL or every emoji, meaning that TTL does not deliver the entirety of the message to a landline phone. Moreover, any translation of text to voice is a "net protocol conversion," which only confirms that the separate TTL offering is also an information service – not CMRS.

[11] *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311, 358 ¶ 80 (2018) (internal quotation marks omitted).

mobile offerings could be deemed a functional equivalent and subject to CMRS regulation.[12] Messaging is not one of them.

First, messaging is functionally different from voice, as reflected in consumer choice. Voice calls do not convey the content that messaging often delivers, from photographs to "clickable" web-links. And messaging does not transmit the real-time, two-way "synchronous" communications of voice.[13] Many consumers prefer text messaging because it provides additional functionality (*e.g.*, the ability to retrieve and review the contents of past communication) and because it is perceived as less invasive and stressful than the immediacy of voice calls.[14] Thus, it is not surprising that consumers use texting 44 percent more frequently than voice to communicate with friends and family multiple times a day.[15]

Second, from a regulatory perspective, it would make no sense to treat OTT messaging, email, and SMS differently. As but one example, Apple's iOS Messages application supports both iMessage and SMS. Messages are sent through Apple's iCloud or the SMS platform depending on whether the recipient is using an iOS or non-iOS device. While each service offers slightly different features, consumers perceive the message as a simple communication, whether sent and delivered as an SMS or iMessage.[16] If anything, text messaging is the

---

[12] *Implementation of Sections 3(n) and 332 of the Communications Act, Regulatory Treatment of Mobile Services*, Second Report and Order, 9 FCC Rcd 1411, 1447 ¶ 79 (1994).

[13] Whereas voice communications response is nearly instantaneous (in the milliseconds), surveys have found that the average time to reply to a text message sent was just over six minutes. *See* Agathe Battestini, Vidya Setlur, and Timothy Sohn, *A large scale study of text-messaging use* (2010), available at https://www.researchgate.net/publication/221270858_A_large_scale_study_of_text-messaging_use.

[14] *See, e.g.*, OpenMarket, *'Shoot Me a Text:' Why Millennials Prefer Text Over Talk* (May 5, 2016), https://www.openmarket.com/blog/millennials-prefer-text-over-talk/.

[15] Memorandum from Morning Consult to CTIA (Nov. 18, 2016) (on file with the author) (Morning Consult Poll) (detailing a November 11-12, 2016 national sample poll of 2,000 registered voters weighted to approximate a target sample of employed adults based on race/ethnicity, gender, educational attainment, and region, with a margin of error of plus or minus 3 percentage points).

[16] Rick Broida, CNET, *Why some iMessage texts are blue and some are green; Admit it: You've always wanted to know* (June 8, 2017), https://www.cnet.com/how-to/why-some-imessage-texts-are-blue-and-some-are-green/.

functional equivalent of OTT messaging or email, and no commenter has suggested that email or OTT messaging are functional equivalents of CMRS.

Messaging-Based Mobile Two-Factor Authentication Helps to Protect Consumers from Fraud

As the Commission continues to evaluate ways to authenticate traffic on the PSTN to mitigate unwanted and illegal robocalls, the Commission should consider the increasingly important role that text messages play in strengthening safeguards that protect consumer privacy and financial transactions. Partnering with the wireless industry, Mobile Two-Factor Authentication (M2FA) was developed with financial, retail and government entities to authenticate consumers. M2FA helps these entities establish whether a consumer's mobile device is in a particular customer's possession in order to identify, authenticate and authorize transactions. For example, through M2FA, wireless providers can validate consumer's identities and locations when roaming outside of the U.S. to ensure that foreign transactions are legitimate. Text message based M2FA has become essential to mitigate online security risks by harnessing the fact that a text message sent to a mobile wireless device is unique to an individual, and travels with a person wherever they go. Through messaging, wireless providers and online security stakeholders are continuing to evolve their solutions to mitigate evolving security threats and protect consumers from fraud.

Source: Morning Consult Poll

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed in ECFS and provided to the Commission participants. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Matthew Gerst
Matthew Gerst
Assistant Vice President, Regulatory Affairs

cc: Suzanne Tetreault
Garnet Hanly
Elizabeth McIntyre
Eli Johnson
Darrel Pae
Jennifer Salhus
Becky Schwartz